

REMARKS

Status of claims

Claims 29 – 53, 57 and 58 are pending, of which 29, 57 and 58 are independent. Claims 29, 57, 58 are currently amended.

To more clearly distinguish the present invention from all cited references and prior art, independent claims 29, 57 and 58 have been amended by the expression "remote" in the feature c "at a remote authorization authority (HA)".

This limitation is described on page 4, lines 4 – 5 and lines 14 – 15, and it is also shown in Fig. 1 – 10 of the present application.

New amended claim 29 is repeated here with features a – g2 set out for convenient reference:

features

- a A method for the initialization of mobile data carriers (IM) with assigned decentralized read and write stations (WR) and/or of decentralized read and write stations (WR) within the frame of an authorization system (A)
- b wherein initialization data (DI, A-I, I-I) are generated in an authorization process in a secure environment (g)
- c at a remote authorization authority (HA)
- d by means of authorization means (AM)
- e and said initialization data are sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)
- f1 to a decentralized authorized read and write station (A-WR)
- g1 where the mobile data carriers (IM) are initialized (IMj) with the initialization data (DI)
- f2 and/or that the initialization data (DI) are sent over the network (N) to a decentralized read and write station (WR),
- g2 by means of which the read and write station is initialized (WRk).

According to **feature a** the present invention discloses a method for the initialization of mobile data carriers (IM) with assigned decentralized read and write stations (WR) and/or of decentralized read and write stations (WR) within the frame of an authorization system (A).

This corresponds to the nearest prior art as it is described in the cited reference WO 97/34265 which is a counterpart to US 6,126,078 (Locher et al.)

Here this initialization must be carried out in a secure (central) environment by a special authorization means. It is not possible to initialize decentralized read and write stations and data carriers in an unsecured environment.

The objective of the present invention is therefore to create a method for initialization of data carriers and decentralised read and write stations in an unsecured environment (from outside).

This objective is achieved by a method according to the additional new and inventive **features b, c, d, e, f1, g1, f2, g2**.

This initialization can relate to application-specific data and to system-specific data and the initialization data DI can include authorization information A-I and initialization information I-I. The initialization process is extensively explained in the examples and for the figures of the description.

Cited References

The cited references Eberhard (5,473,689) and Sciupac (US 6,871,278) cannot present a nearest prior art, since they do not disclose an initialization process and especially not a method for initialization of decentralized read and write stations (WR, A-WR) and data carriers (IM) from a remote authorization authority (HA).

The objects of these references are entirely different as compared to the object of the present invention.

Reference Eberhard discloses a new method for mutual authentication between a first electronic device (a read and write station) and a second electronic device (a mobile data carrier) for communication with improved security. This method is including an encryption with two random numbers generated in the first electronic device.

Reference Sciupac discloses a transaction system for secure communication and authentication between a read and write station 10 and a data carrier 12 and a host computer 14. The read and write station stores cryptographic keys and firmware for executing the secure protocols.

In principle these cited references only deal with a first step: the authentication and establishing of a secure communication, and not with a second step of initialization.

Whereas in the present invention after such a first step of authentication and establishing of a secure communication between the four elements: authorization medium (AM), authorization authority (HA), read and write stations (A-WR, WR) and data carrier (IM) in a second step the inventive initialization is carried out in the secured communication.

Claim Rejections – 35 USC 102

The independent claims 29, 57 and 58 are rejected as being anticipated by reference Eberhard (US 5,473,689). The examiner cites column 3, lines 3 to 36 to disclose the content of claim 29. But not in this passage, nor in the entire description of Eberhard, is a method of initialization according to the features b – g2 of claim 29 as underlined are disclosed or indicated:

features

- a A method for the initialization of mobile data carriers (IM) with assigned decentralized read and write stations (WR) and/or of decentralized read and write stations (WR) within the frame of an authorization system (A)
- b wherein initialization data (DI, A-I, I-I) are generated in an authorization process in a secure environment (g)
- c at a remote authorization authority (HA) (3. element)
- d by means of authorization means (AM) (4. element)
- e and said initialization data are sent over a network (N) in a secure communication according to security rules corresponding to the authorization system (A)
- f1 to a decentralized authorized read and write station (A-WR) (1. element)
- g1 where the mobile data carriers (IM) are initialized (IMj) with the initialization data (DI) (2. element)
- f2 and/or that the initialization data (DI) are sent over the network (N) to a decentralized read and write station (WR),
- g2 by means of which the read and write station is initialized (WRk).

As an example, the random numbers Z1, Z2 of Fig. 2 in Eberhard are not initialization data (DI, A-I, I-I). They only serve for the encryption in the mutual authentication of the two electronic devices:

1. read and write station
2. mobile data carrier

These random numbers cannot contain any message.

Further: The inventive method includes the four system elements:

1. read and write station (WR, A-WR)
2. data carrier (IM)
3. remote authorization authority (HA)
4. authorization means (AM).

Eberhard deals only with a

1. element = first electronic device (WR) and a
2. element = second electronic device (IM)

There is no third and no forth element in Eberhard.

The cited references of Eberhard and Sciupac as well as a further cited prior art do not disclose the new and inventive method for initialization according to the features and limitations of present claims 29, 57 and 58.

Even with a combination of these references, there is no indication of these new features of the present invention.

Therefore the independent claims 29, 57 and 58 should be allowable and with it also the depending claims.

Reconsideration is requested.

Respectfully submitted,

/s/

Carl Oppedahl
PTO Reg. No. 32746